تروریسم سایبری و حقوق بشر دوستانه بین المللی

سیما حاتمی* [۱]
فتح اله رحیمی[۲]
اسماعیل شاهسوندی[۳]

تاریخ دریافت:۱۴۰۱/۱۰/۰۱ تاریخ پذیرش:۱۴۰۱/۱۲/۲۹

چکیده

سایبرتروریسم با هدف ممانعت از دسترسی به اطلاعات و ایجاد اغتشاش و برهم زدن امنیت ملّی و بین المللی برای طرف های درگیر با ایجاد رعب و وحشت در دنیای کنونی و با فناوری فوق پیشرفته مطرح است و مراکز حیاتی، حساس و مهم را تحت تاثیر قرار می دهد. توجّه و پرداخت سریع و در عین حال هوشمند، هدفمند و معقول به موضوع بمنظور مصون سازی این مراکز از تهدیدات موجود و محتمل الوقوع در جهت حفظ امنیت ملّی و حریم شخصی شهروندان در عرصه نبرد سایبری ضروری است. سایبر تروریسم و رابطه آن با حقوق بین الملل در قالب حقوق مخاصمات بین المللی و حقوق بشردوستانه محور مطالعه این جستار تحقیقی و تحلیلی است. رویکرد استقرایی بکار رفته در تحلیل موضوع، مبیّن آن است که ماهیت سایبر تروریسم در حقوق بین الملل ذیل حقوق بشردوستانه تعریف می شود و تمهیداتی را برای مقابله با آن توسط دولت ها ارائه می دهد .

واژگان کلیدی :سایبرتروریسم، فناوری اطلاعات، حمله سایبر، حقوق مخاصمات، حقوق بشردوستانه

۱-دانش آموخته دانشکده حقوق و علوم سیاسی دانشگاه تهران (نویسنده مسئول)drsimahatami@gmail.com
۲-عضو هیات علمی دانشگاه آزاد اسلامی واحد تهران شمالrahimif_law@yahoo.com
۳- عضو هیات علمی دانشگاه آزاد اسلامی واحد تهران شمال es.shahsavandi@ymail.com

۱-مقدمه

بی شک، تروریسم[1] در جهان معاصر با حادثه ۱۱سپتامبر ۲۰۰۱ در حمله به برج های دو قلوی تجارت جهانی به نقطه اوج رسید. البتّه تروریسم بسیار قبل تر از آن وجود داشت، بگونه ای که از هجده سند بین المللی (شامل اصلاحیه ها و متمم ها[2]) که از سال ۱۹۶۳ به تصویب رسیده، سیزده سند مربوط به قبل از سال ۲۰۰۱ است.

تحوّل تدریجی اصول کلّی حقوق بین الملل[3] مربوط به تروریسم، از ۱۱ سپتامبر، بنظر می رسد حالت یک طرفه ای دارد؛ زیرا علیرغم آنکه برخی از عناصر مربوط به آن، آنچنانکه در عدم پذیرش کنوانسیون جامع تروریسم بین المللی[4] و عدم ارائه تعریف تروریسم متبلور است، به هیچ وجه تغییر نکرده اند؛ لیکن سایر عناصر مرتبط با تروریسم، به شدّت تغییر یافته و متحوّل شده اند. به رسمیت شناختن صریح حق دفاع یک کشور در پاسخ به یک حمله تروریستی در قطعنامه های شماره ۱۳۶۸ و ۱۳۷۳ شورای امنیت سازمان ملل متّحد**(UNSC)**[5] مصداقی از این مدعا است(**Derek Jinks; 2003; 32**)

بهرحال، توجّه به مبانی قانونی دفاع در برابر حمله تروریستی سایبری که به آستانه حملات ۱۱ سپتامبر می رسد، ضروری است. برخی بر این باورند که هیچ تهدید سایبری قریب الوقوعی وجود ندارد{ **Massimo Mauro; 2006; pp 219, 221 (Edward Halpin et al. eds., 2006)** **;**}.[6] معذالک، اگرچه حملات سایبری هنوز به طور رسمی رکوردی را از نظر تلفات شدید ثبت نکرده اند؛ اما شکاف بزرگ و عمیقی بین خطر مفروض و فعالیت‌های تروریستی سایبری، شناسایی شده است(**Anna-Maria Talihärm; 2010; pp 59, 62**). با اینحال، بموازات تکامل سریع فناوری‌های نوین و فوق العاده، مدت مدیدی است که تروریسم سایبری نیز بعنوان تهدیدی برای حیات و زندگی بشر شده است.

بهر صورت، این جستار تحلیلی در صدد پاسخ به این پرسش اساسی است که ارتباط سایبر تروریسم با حقوق جنگ یا بعبارتی صحیح تر حقوق بشردوستانه بین المللی چیست و چه رژیم حقوقی بر آن حاکم است؟ در این راستا، بنظر می رسد با استقراء در رویه دولتها و تحلیل اسناد بین المللی مربوطه می توان بیان داشت که تروریسم سایبری نیز با ابتنای به توصیف تروریسم بعنوان «هرگونه اقدام، علاوه بر اقدامات

[1]-Terrorism
[2]-International Legal Instruments to Counterterrorism, U.N. Action to Counterterrorism, http://www.un.org/terrorism/instruments.shtml (last visited Aug. 21, 2012).
[3]-General principles of international law
[4]- The UN Comprehensive Convention on International Terrorism
[5]-Tthe United Nations Security Council (UNSC) in Resolutions 1368 and 1373
[6]-Also See Dorothy Dennings, A View of Cyberterrorism Five Years Later, in Redings in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed., 2006), cited in Eneken Tikk, Comprehensive Legal Approach to Cyber Security, 35 Dissertations Juridical Universities Taruensis 22 (2011).

مشخص شده در کنوانسیون‌های ژنو و قطعنامه ۱۵۶۶ (۲۰۰۴) شورای امنیت، که به منظور مرگ یا ایراد صدمات جدّی بدنی به غیرنظامیان یا غیرنظامیان صورت بپذیرد، موضوعی است که حساسیت بین المللی را در پی دارد و با تفکیک عمل نظامیان در استفاده از فناوریهای روز در فضای سایبر در حمله به دشمن بعنوان عمل نظامی از عمل افراد و گروههای تروریستی که با استفاده از فناوری الکترونیکی در فضای سایبر با اختلال در سیستمهای هوشمند شهری و تخریب عمده زیرساختهای حیاتی و حساس یک کشور، موجب رعب و وحشت مردم و وادار کردن دولت به انجام یا عدم انجام کاری می شوند، چنانچه میزان و شدّت حمله سایبری به آستانه حمله مسلّحانه برسد، تحقیقاً مشمول قواعد حقوق مخاصمات مسلّحانه خواهد بود. لذا محور ساخت چنین توصیفی از تروریسم سایبری نیز آن است که هدف از آن، بنا به ماهیت یا زمینه عمل ارتکابی، ارعاب جمعیت یا مجبور کردن دولت یا سازمان بین المللی به انجام یا خودداری از انجام هر عمل غیر قانونی می باشد.

۲- ظهور تروریسم سایبری و سطح بندی ساختاری آنها

در طول جنگ سرد، در رویکردی واقع‌گرایانه از روابط بین‌الملل، دولتها در کانون اصلی توجّه قرار داشتند و متعاقب ظهور «دولت امنیت ملّی»، به سبب خطرات ناشی از مسابقه تسلیحات هسته ای و ترس از آن، مبادرت به ایجاد دستگاه های امنیتی و اطلاعاتی قدرتمند نمودند(راسکین، ۱۹۷۶)[1]. اما با تحوّلات روابط بین الملل در اواسط تا اواخر دهه ۱۹۸۰، انواع بازیگران غیردولتی، از جمله گروه‌های تروریستی و سازمان‌های بین‌المللی در کانون توجّه قرار گرفتند و دیگر، دولتها همانند قبل، در روابط نوظهور بین المللی، «جعبه سیاه» نبودند. در این تغییر، اینبار آنچه در داخل دولت اتفاق افتاد، نیز در شکل‌دهی امور بین‌المللی مهم بود؛ لذا طیف جدیدی از نظریه‌های بین‌المللی، با تمرکز بر بازیگران خرده دولت، گروه‌های هویتی و پویایی‌های اجتماعی ابراز شدند (بوزان، ۱۹۹۱[2])

نظر به اینکه در حال حاضر بیش از صد سازمان تروریستی بین‌المللی از گروه‌های کوچکی نظیر فیانا عایران، حرکت‌الجهاد الاسلامی، مجاهدین خلق ایران که توسط چند کشور تعیین شده‌اند تا گروه‌های گسترده تری نظیر القاعده، لشکر طیبه، اسباط الانصار، داعش و غیره که بعنوان سازمان تروریستی شناخته می‌شوند؛ در جهان مدرن امروز، پناهگاه‌های امن سایبری زیادی ایجاد کرده اند که این گروه‌ها می‌توانند بدون ترس از انتقام‌جویی مستقیم، در آنجا فعالیت کنند{ **Stuart H. Starr; 2009; 18, 34 (Christian**

[1]- Cited in Simona R. Soare, Joe Burton Smart Cities, Cyber Warfare and Social Disorder, [UNDATED].
[2]- Ibid.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

Czosseck & Kenneth Geers eds., 2009)}.[1] البتّه بنظر می رسد موفقیت دولتها در عملیات ضد تروریستی، احتمالاً این بازیگران غیردولتی را به تروریسم سایبری سوق داده، بنحوی که برخی گروه ها که پناهگاه فیزیکی خود را در مناطق کلیدی و مهم از دست داده اند، به پناهگاه های فضای مجازی روی آورده اند.(**Gabriel Weimann; 2004, at 1, 11**). با اینحال، از لحاظ ساختاری، می توان قابلیتهای تروریسم سایبری این سازمانهای تروریستی را آنچنانکه مرکز مطالعه تروریسم و جنگ های نامنظم در دانشکده تحصیلات تکمیلی نیروی دریایی در مونتری در سال ۱۹۹۹ تبیین کرده، در سه سطح مشخصِ ساختار ساده[2]؛ ساختار پیشرفته[3] و ساختار پیچیده[4] توصیف کرد.

الف-ساختار ساده؛

این ساختار، علیرغم آنکه توانایی انجام اقدامات هک اساسی علیه سیستم های فردی با استفاده از ابزارهایی که توسط شخص دیگری ایجاد شده را دارد؛ مع الوصف، واجد سازمان تحلیل هدف، فرماندهی و کنترل، یا توانایی یادگیری بالایی نیست.

ب.ساختار پیشرفته:

ساختاری است که قابلیت انجام حملات پیچیده تر علیه چندین سیستم یا شبکه و احتمالاً اصلاح یا ایجاد ابزارهای هک اساسی[5] را دارد و یک سازمان واجد تجزیه و تحلیل هدف اولیه، فرماندهی و کنترل و قابلیت یادگیری است.

ج.ساختار پیچیده

این ساختار تروریستی، قابلیت حملات هماهنگ جهت ایجاد اختلال انبوه در برابر دفاع های یکپارچه و ناهمگن، از جمله رمزنگاری[6] می باشد و امکان ایجاد ابزارهای پیشرفته هک با توانایی بالا را دارد و واجد مکانیزم تجزیه و تحلیل هدف، فرماندهی و کنترل و قابلیت یادگیری سازمانی است(**Bill Nelson; 2000; 23**).

مستندات دلالت دارد که القاعده در سال ۲۰۰۲ در صدد یک حمله سایبری به یک سد(**Shima D. Keene; 2011; pp 359, 364-65**) و در سال ۲۰۰۵ قصد از بین بردن کل ترافیک اینترنت بریتانیا را

[1]- Also See. Kenneth Geers, Cyber Weapons Convention 26 Computer L. & Sec. Rev. 547 (2010). Also, Gabriel Weimann, Cyberterrorism: How Real Is the Threat? U.S. Inst. of Peace, Dec. 2004, at 1, 11.
[2]- Simple-Unstructured
[3]- Advanced-Structured:
[4]- Complex-Coordinated3.
[5]- Basic Hacking tools
[6]- Cryptography

داشت و یا حامیان ببرهای آزادی بخش تامیل ایلام[1] ایمیل‌هایی را با هدف مختل کردن ارتباطات به سفارت‌های مستقر در سریلانکا ارسال کرده‌اند (**Id. at 363**).

روشهای تروریستها در ساختارهای مذکور، در جهت تقویت فعالیتهای مربوط، قابل توجّه است. در فضای سایبر و تروریسم سایبری فی نفسه، سطح پایین تخصص فنّی در ساختارهای (ساده- و حتّی بدون ساختار) با بکارگیری افراد ماهر از نظر فنّی و گاهی هم بهبود قابلیت های تروریست ها ارتقاء می یابد(**Bill Nelson; 2000; 23**). لذا گروه‌های کوچک مجرمان سایبری ممکن است با یکدیگر همکاری نموده و حتّی چنانچه دیدگاه‌های رادیکال مذهبی یا اجتماعی-سیاسی مشابهی با سازمان‌های تروریستی شناخته شده، داشته باشند، با آنها ادغام شوند(**Clay Wilson, Botnets; 2008; 18**). ضمن آنکه افراط گرایان می توانند با پرداخت هزینه، دانش و برنامه های لازم را از تیم های هکر دریافت کنند. برخی از گروه‌ها مانند «انجمن هکرهای روسیه» خدمات یکبار مصرف را از طریق اینترنت ارائه می‌دهند.[2] با اینحال، امروزه اطلاعات مربوط به آسیب‌پذیری رایانه‌ای، که هنوز نرم‌افزاری هم برای رفع مشکلات آنها طراحی نشده، در بازار سیاه با پرداخت مبلغی بین ۱۰۰۰ تا ۵۰۰۰ دلار آمریکا[3] قابل دریافت است.

برخی از گروه‌های مجرم سایبری ممکن است با «تروریست‌های میدانی[4]» دارای همپوشانی اهداف باشند؛ لیکن بعضاً نیز ترجیح می‌دهند مستقل عمل کرده و سعی کنند در «تروریسم سایبری محض[5]» شرکت نمایند. به عنوان مثال، گروه «جی-فورس پاکستان» (هواداران القاعده)[6] با هدف آزادسازی کشمیر، یک کمپین مستقل نفوذی علیه جامعه اینترنتی به راه انداخت که در سال‌های ۲۰۰۱ تا ۲۰۰۲ به اوج خود در باب آزادسازی کشمیر رسید؛ اگرچه فعالیت‌های این گروه، بیشتر شامل تخریب وب‌سایت‌ها بود، نه صرفاً اقدامات واقعی تروریسم سایبری.

برخی معتقدند که اقدامات تروریستی سایبری علیه این اهداف برای سازمان‌های تروریستی نسبت به یک حمله معمولی، مطلوب تر نیست؛ زیرا منجر به تأثیر روانی کمتری می‌شود. جریحه دار کردن احساسات عمومی و خدشه به امنیت جمعیتی و بر هم زدن آرامش انسانها نیز در این زمینه حائز اهمیت است. این موضوع در بحران گروگانگیری نورد اوست در مسکو (۲۰۰۲)، بمب گذاری های مادرید (۲۰۰۴)، بمب گذاری های لندن (۲۰۰۵) و سایر حملات تروریستی مشهود است(**Gordon & Ford, 2003**). با اینحال، بر خلاف تروریسم سنّتی، تروریسم سایبری برای موفقیت، نیازی به سرمایه گذاری مالی قابل توجّه و

[1]- Tigers of Tamil Eelam
[2]- Nick Ellsmore, Cyber-Terrorism in Australia: The Risk to Business and A Plan to Prepare 7 (2002).
[3]- Black market for a sum of $1,000 to $5,000 USD.
[4]- "Field-Terrorists,"
[5]- "Pure cyberterrorism
[6]- The "G-Force Pakistan" group (sympathizers of Al-Qaeda)

یا حضور فیزیکی ندارد. در واقع، تنها پیش نیاز لازم برای انجام یک عمل تروریستی سایبری، دانش فنّی است که پس از کسب آن، یک دارایی رایگان و قابل استفاده مجدد خواهد بود؛ در غیر اینصورت، انجام عملیات تروریستی برای افراط گرایان مشکل و پر هزینه خواهد بود.

اگرچه رژیم معاهداتی کنونی مربوط به تروریسم، مستقیماً به حملات سایبری اشاره نمی‌کند و اکثر کنوانسیون‌های موجود نیز در دورانی ایجاد شده‌اند که حملات سایبری غیرقابل تصور بوده، لیکن این امر کاربرد آنها را برای اقدامات تروریستی سایبری منتفی نمی‌کند؛ ضمن آنکه اصول مندرج در آنها در شکل گیری حقوق عرفی بین المللی در رابطه با این أعمال مؤثر است(**Matthew J. Skleroy; 2009; PP 64-65**). لذا از آنجا که در زمینه تروریسم سایبری، تمایز بین خطرات واقعی و سناریوهای با احتمال کم، که نزدیک به واقعیت هستند، مهم می باشد، از لحاظ تحلیلی، محتوای اسناد حقوقی بین المللی مذکور، دلالت بر این دارد که افزایش امکان ارتکاب اقدامات تروریستی جرم انگاری شده از طریق فضای سایبری، به ترتیب از غیرممکن تا بسیار محتمل خواهد بود.

۳. شهرهای هوشمند[1] و سایبر تروریسم

آرام آرام، تحوّلات مستمر ناشی از پیشرفتهای تکنولوژیکی بشری، توجّهات را به شهرها معطوف نمود. در این راستا البتّه دو گرایش نوظهور باعث شد تا شهرها در تحلیل روابط بین المللی مورد توجّه قرار گیرند. روند اول معطوف به پدیده جهانی شدن است که ارتباط سیاسی، مالی و نظامی شهرها و نقش آنها را به عنوان مرکز فرماندهی و برنامه ریزی ارتقاء داد (آلدرسون و همکاران، ۲۰۰۶[2]). ترکیب اثرات جهانی شدن و گسترش سریع فناوری اطلاعات و ارتباطات، جهان را «مسطح» کرد و با تغییرات جهانی، تأثیر و تأثر وضعی متقابل داشت. روند دوم مربوط به شهرنشینی است، فرآیندی که با جهانی شدن، افزایش بازارهای بین المللی، صنعت، ظهور اقتصادهای خدمات محور و فرصت های شغلی، و کاهش زندگی و اقتصاد روستایی انجام شده است. از سال ۲۰۱۶، بیش از نیمی از جمعیت جهان در شهرها زندگی می‌کنند و قرار است این رقم تا سال ۲۰۵۰ به دو سوم یعنی حدود ۷ میلیارد نفر افزایش یابد (ریچی و روزر، ۲۰۱۸[3]).

شهرها از آن جهت که واجد چندین کارکرد مهم سیاسی، اقتصادی و امنیتی هستند، مدیریت آینده شهرنشینی، از جمله پایداری زیست‌محیطی، اقتصادی و اجتماعی، برای امنیت شهری، مهم و حیاتی خواهد بود. امروزه حتّی برخی از شهرها از حیث اینکه مراکز اصلی اقتصادی هستند؛ کمااینکه بازارهای سهام

[1]- Smart Cities
[2]- Cited in Simona R. Soare, Joe Burton Smart Cities, Cyber Warfare and Social Disorder, [UNDATED].
[3]- Ibid.

جهانی،[1] که اکنون تحت تسلط نیویورک، هنگ کنگ، لندن و توکیو قرار دارند، میزبان زیرساخت‌های مالی جهانی و نهادهای اداره کننده اقتصاد جهانی هستند، لذا در صورت حمله سایبری به آنها، کل اقتصاد دنیا در طرفه العینی خواهد خوابید.[2]

شهرها همچنین مراکز اصلی دیپلماتیک و روابط سیاسی جهانی هستند و سفارتخانه ها، کنسولگری ها و منافع خصوصی بی شماری برای نفوذ سیاسی در شهرها قرار دارند؛ لذا فی حد نفسه به بازیگران مهمی تبدیل شده‌اند که عاملی در حال رشد در امور بین‌الملل می باشند. علاوه بر این، شهرها محل گذارهای سیاسی عمده ای مانند بهار عربی بوده و میزبان مکان های دیدنی نمادین مانند برج ایفل، بیگ بن، مرکز تجارت جهانی وان، پل بندرگاه سیدنی و برج خلیفه هستند که اهمیت سیاسی و امنیتی گسترده ای دارند. لذا حفظ امنیت آنها در مقابل حملات سایبری، حائز اهمیت است.

۲-۱- ظهور شهرهای هوشمند و ضرورت دفاع

شهرهای هوشمند، بطور مؤثر سیستم های فیزیکی، دیجیتالی و انسانی را در محیط های شهری برای ارائه نتایج پایدار، فراگیر و مرفه برای شهروندان خود یکپارچه می کنند.[3] در حال حاضر، مطمئناً در شهرها فناوری وجود دارد، اما أشکال کاملاً یکپارچه و خودکار کنترل فناوری بر خدمات مختلف و افرادی که از آنها استفاده می‌کنند، هنوز در حال توسعه است. نیل به نتایج مثبت در این زمینه، به امنیت شهر هوشمند بستگی دارد؛ کمااینکه اکنون آسیب‌پذیری‌های تکنولوژیکی پروژه‌های احداث شده در شهر هوشمند نیز مورد توجّه است. وابستگی فزاینده شهرهای هوشمند به اتصالات فناوری و داده ها، آسیب پذیری های آنها را در برابر حملات سایبری و تهدیدهای نفوذ هیبریدی خارجی افزایش می دهد. لذا شهرهای هوشمند در معرض حملات سایبری و آسیب های واقعی و جدّی ناشی از آن هستند و از این جهت، می توانند مکان امنی برای مردم باشند.

سطوح حمله چندگانه به یک شبکه شهر هوشمند، حتّی می تواند موجب نگرانی فزاینده در مورد تهدید حقوق مدنی و سیاسی شهروندان شود(سوخاک و همکاران، ۲۰۱۹[4]). ضمن آنکه همواره ممکن است چالش‌های امنیتی درباره حملاتی که باعث اختلال در خدمات و سرقت یا دستکاری داده‌های جمع‌آوری‌شده توسط حسگرها می‌شوند، وجود داشته باشد(**Elmaghraby & Losavio, 2014**).

[1]- Cosmopolitans
[2]- Statista.2020
[3]- British Standards Institute. (2014) PAS 181 Smart city framework. Available from: https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/ [Accessed 28th August 2020].
[4]-Ibid

زیرساخت های هوشمند در یک شهر هوشمند اعم از حمل و نقل عمومی و کنترل ترافیک، شبکه انرژی، تامین آب، مدیریت زباله، عملیات ساختمانی، مراقبت‌های بهداشتی، سیستم‌های تحویل کالا، خدمات اداری محلی، سیستم‌های پشتیبان و غیره معمولاً توسط یک شبکه مُرکّب و هم افزایی از زیرساخت های فیزیکی و مجازی فعال می شوند که نحوه تعامل شهروندان با مدیریت شهری و حکومت محلی را مشخص می کند. لذا اگرچه روند توسعه بنحوی است که در آینده نزدیک شبکه‌های متصل به جی فایو (جی-۵) اینترنت اشیاء و شبکه‌ها و پلتفرم‌های خدمات مستقل (سرویس‌های الکترونیکی که بصورت خودکار و با حضور انسان عمل می کنند) می توانند طراحی، عملیات و کارایی شهر هوشمند را در دهه ۲۰۲۰ متحوّل و اصلاح کنند؛ لیکن هر یک از اجزای زیرساخت شهر هوشمند آسیب‌پذیری خاص خود را دارد، کمااینکه سیستم‌های پیچیده، چند لایه و بهم پیوسته در زیرساخت شهر هوشمند، بطور سیستمی در برابر تعداد فزاینده‌ای از تهدیدات از جنایات سایبری تا جنگ ترکیبی آسیب‌پذیر هستند.

آگاهی روزافزون نسبت به خطرات امنیت سایبری نهفته در زیرساخت های شهر هوشمند و اثرات فیزیکی بالقوه آنها و دفاع در مقابل آنها بجای ریسک گریزی، یکی از مولّفه های مدیریت ریسک است. پیش‌بینی می‌شود هزینه‌های امنیت سایبری برای زیرساخت‌های شهر هوشمند بین سال‌های ۲۰۲۰-۲۰۲۴ به بیش از ۱۳۵ میلیارد دلار افزایش یابد.[1]

طراحی امنیت سایبری و حفظ آن، ملازم توسعه طرح‌های شهر هوشمند است. استانداردسازی و صدور گواهینامه، از جمله استانداردهای ایزو[2] برای شهرهای هوشمند و گواهینامه اتحادیه اروپا برای دستگاه ها و خدمات[3]، وضع مقررات خاص برای حفاظت از زیرساخت های حیاتی که مقامات ملّی و اپراتورهای خدمات شهر هوشمند باید از آن پیروی کنند،در زمره این طرح ها می باشد. از آنجاکه اجرای این استانداردها و مقررات، یک مزیت ملّی است، لذا تفاوت در تمرکز استراتژیک به موضوع، سطح ظرفیت فناوری و تخصیص بودجه برای این مهم، مبیّن سطوح مختلف عملکرد است.

۴- عناصر مقابله با سایبرتروریسم در حقوق مخاصمات [4]

الف- دفاع از خود در برابر تروریسم

امروزه دولت‌ها از آسیب‌پذیری‌های زیرساخت‌های داخلی و تهدید بالقوه‌ای که تروریسم سایبری برای آنها دارد، آگاهند. با اینحال، همکاری بین الدولی در مقابله با تروریسم، به نوعی عقیم باقی مانده است؛ کما

[1]- ABI Research; 2019
[2]- ISO Standards
[3]- ICT (EC 2020)
[4]- Jus Ad Bellum

اینکه کارگروه اجرای مبارزه با تروریسم سازمان یافته، هنگامی که در مورد مقابله با استفاده از اینترنت برای اهداف تروریستی[1] از کشورها درخواست کرد تا در سال ۲۰۰۹ گزارشی ارائه کنند، تنها دو کشور حملات سایبری توسط تروریست ها را بعنوان تهدیدهایی که آنها را نگران می کرد، گزارش کردند.[2] این وضعیت، با توسعه سریع قابلیت های دفاع و تهاجم سایبری توسط ایالات متّحده، چین، روسیه، ایران، کوبا، اسرائیل، بریتانیا و دیگران در تضاد است(**W.P. Strobel; 2000; 32**) و نشان می دهد که این کشورها به دنبال استفاده از آنها هستند و حقّ دفاع فردی از خود در برابر تروریست های سایبری، بر اقدام جمعی در آینده، ارجح بوده و برای دولتها موضوعیت دارد.

در واقع، دو دولت، یعنی اسرائیل و ایالات متحده، به خاطر رویه مستمرشان در استفاده از زور علیه تروریست‌ها و دولت‌هایی که آنها را پناه می‌دهند، در این زمینه متمایزند و در حالیکه شورای امنیت، طی قطعنامه های متعدد، عملیات «دفاع از خود» در برابر حملات تروریستی قبلی مانند حمله به فرودگاه بیروت در سال ۱۹۶۸ (قطعنامه ۲۶۲)، یورش به لبنان در سال ۱۹۷۳ (قطعنامه ۳۳۲ و ۳۳۷)، بمباران مقر ساف در تونس در سال ۱۹۸۵ (قطعنامه ۵۷۳) و ترور خلیل الوزیر در سال ۱۹۸۸ (قطعنامه ۶۱۱)، را محکوم نموده، لیکن اسرائیل همچنان بر موضع خود مبنی بر تفسیر گسترده حق دفاع از خود پافشاری می کند و احتمالاً این کار را در رابطه با تروریسم سایبری هم ادامه خواهد داد(**Christine Gray; 2000; 116**) .

اگرچه به نظر می‌رسد استدلالات اسرائیل در این زمینه، جامعه بین‌المللی را متقاعد نکرده، اما پس از یازده سپتامبر، دولت‌ها به صراحت امکان اقدام در دفاع از خود در برابر سازمان‌هایی مانند حزب‌الله و حماس را رد نمی‌کنند و ترجیح می‌دهند بجای آن در ارزیابی قانونی بودن حمله هوایی در نزدیکی دمشق در سال ۲۰۰۳، تهاجم به لبنان در سال ۲۰۰۶، و بمباران غزه در ۲۰۱۲-۲۰۰۷ بر مسائل تناسب در دفاع، تمرکز کنند.

البتّه محکومیت اقدام ایالات متحده در «دفاع از خود» در برابر تروریست ها در شورای امنیت به دلیل وتوی آمریکا، محتمل نبود. با این وجود، مجمع عمومی سازمان ملل متحد موفق شد بموجب قطعنامه ۳۸/۴۱ بمب گذاری جاماهریای لیبی در سال ۱۹۸۶ را که در واکنش به بمب گذاری دیسکوتک برلین انجام شد، را محکوم نماید. عملیات «ضد تروریستی» ایالات متحده در عراق در سال ۱۹۹۳ و همچنین در سودان و افغانستان در سالهای ۱۹۹۸ تا سال ۲۰۰۱ نیز مواردی بودند که شورای امنیت در قطعنامه ۱۳۶۸ خود بطور تلویحی پرسش های حقوقی مبنی بر اینکه ایالات متحده از این حق برخوردار است، را مطرح کرد.

[1]- UN Counter-Terrorism Implementation Task Force (CTITF) Working Group on Countering the Use of the Internet for Terrorist Purposes.
[2]- U.N .Counter-Terrorism Implementation Task Force , Report on Countering the Use of the Internet For Terrorist Purposes 3 (Feb. 2009), available at http:// www.un.org/en/terrorism/ctitf/pdfs/ctitf_internet_wg_2009_report.pdf.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

توسّل به دفاع از خود در برابر یک سازمان تروریستی، در نوع خود طلیعه دار پرسش های عدیده ای است که بی شک بدون پاسخ مانده اند. این امر با تأیید بی‌صدای جامعه بین‌المللی در مورد تهاجم به افغانستان در سال ۲۰۰۱ و نیز با رویکردهای قانونی اتخاذ شده در خود ایالات متّحده تأیید شد(**Raphaël; 2010; pp183, 193**). در ایالات متحده امریکا، رئیس‌جمهور دارای اختیارات قانونی برای استفاده از نیروهای مسلّح در عملیات نظامی، علیه تروریست‌ها است و لاجرم این امر شامل تروریسم سایبری نیز خواهد بود.

کشورهای دیگر نیز به ماده ۵۱ منشور ملل متحد استناد کرده تا حملات علیه گروه های تروریستی را با بازخوردهای متفاوت توجیه کنند. واکنش‌ها به تهاجمات متعدد ترکیه به شمال عراق در دهه های گذشته برای تعقیب حزب کارگران کردستان از صِرف درک اقدام ترکیه تا نگرانی در این باره متغیّر بود. واکنش نسبت به تعقیب جنگجویان چچنی توسط روسیه در گرجستان، حمله ایران به پایگاه های مجاهدین خلق و گروه های کرد عراقی، مشارکت اتیوپی در جنگ داخلی سومالی در سال ۲۰۰۶ و حمله کلمبیا به خاک اکوادور در سال ۲۰۰۸ برای درگیری با فارک، مصادیقی از رویکردهای متفاوت دولتها نسبت به مواجهه دولتها با تروریستها با استفاده از دکترین دفاع از خود می باشد(**Christian J. Tams; 2009; pp 359, 379**)

اگرچه این قبیل نمونه‌ها مستقیماً معطوف به تروریسم سایبری نیست، لیکن مبیّن این واقعیت حقوقی است که دولت‌ها چگونه ممکن است به حملات سایبری جدّی از سوی بازیگران غیردولتی واکنش نشان دهند. تا به امروز هیچ کشوری به تلاش برای انجام یک حمله سایبری اعتراف نکرده و انتظار می‌رود بازیگران غیردولتی بیشتر در چنین فعالیت‌هایی شرکت کنند. از منظر حقوق بین‌الملل، نامگذاری یک گروه یا سازمان با قابلیت‌های تهاجمی سایبری به عنوان «تروریست» برای جبران خسارات و جلوگیری از تکرار چنین جنایاتی کافی نیست؛ بلکه احتمالاً برنامه ریزی برای راه اندازی یک حمله سایبری به مثابه «توسّل به زور» و عملی غیرقانونی و نوعی «حمله مسلحانه» تلقّی خواهد شد که در اینصورت، مبنایی برای استناد به ماده ۵۱ منشور ملل متحد در توجیه اقدام نظامی در مقام دفاع مشروع خواهد بود.

در پرونده دیوارحائل[1] دیوان بین المللی دادگستری به این نتیجه رسید که «ماده ۵۱ منشور ملل متحد، وجود یک حقّ ذاتی دفاع از خود را در مورد حمله مسلّحانه یک دولت علیه دولت دیگر به رسمیت می شناسد».[2] حقّ دفاع از خود علیه بازیگران متجاوز غیردولتی در حقوق بین الملل عرفی از ازمنه قدیم وجود

[1]- THE WALL CASE
[2]- Legal Consequences of Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J 136, ¶ 128 (July 9) [hereinafter Wall Case]. This conclusion can be considered an example of "unhelpful caution in using the judicial tools at its

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

داشته است. ضمن آنکه همانطور که قاضی هیگینز نیز اشاره کرده، در متن ماده ۵۱ چیزی وجود ندارد که تصریح کند «دفاع از خود» تنها زمانی که یک دولت حمله مسلّحانه انجام دهد، قابل استناد است»(**Yaroslav Shiryaev; 2010; 14**).

لذا در یک رویکرد تحلیلی، حمایت گسترده از قانونی بودن ادعای ایالات متّحده برای دفاع از خود در افغانستان، مؤیّد استظهار آن به استدلال حقوقی دائر بر انطباق آن با مفهوم دفاع مشروع مقرر در ماده ۵۱ منشور ملل متحد نیست و لزوماً نمی تواند با تفسیر مجدد معتبر از منشور، در مقام ظهور حقوق بین‌المللی عرفیِ آنی باشد.

برخی استدلال کرده‌اند که ایالات متحده از شورای امنیت سازمان ملل متحد درخواست تأیید قانونی عملیات نظامی خود در قطعنامه ۱۷۱ را نکرده و بجای آن، برای اجتناب از ایجاد سابقه، به دفاع از خود بصورت انفرادی استناد نموده است. در جهان پر تلاطم و مدرن امروز، دیگر زمان بحث از تحوّل طبیعیِ غیر آنیِ هنجارهای مرسوم سپری شده و امروزه، دیگر این سئوال مطرح نیست که آیا گروه‌های تروریستی (و تروریست‌های سایبری) می‌توانند یک «حمله مسلّحانه» انجام دهند یا خیر؛ بلکه این سئوال مطرح است که تا چه حد لازم است دخالت دولت «برای اجازه استفاده از زور علیه قلمرو کشور میزبان» انجام شود(**Chirstian Henderson; 2010; 158**).

تقابل دو دیدگاه متضاد در حقوق بین الملل در موضوع ماده ۵۱ منشور ملل متحد، مؤیّد ناهمواری استناد به دفاع مشروع در اقدامات مرتبط با ضد تروریستی است. اکثریت قضات دیوان بین المللی دادگستری در پرونده فعالیت های مسلّحانه موافقند که اگر حملات «باندهای مسلّح» قابل انتساب به یک دولت نباشد، هیچ شرایط قانونی برای إعمال حقّ دفاع از خود در برابر آن دولت وجود ندارد. در حالیکه اقلیّت آنها شامل قاضی سیما و کویمانز[1] بر این باورند که «حملات مسلّحانه....توسط باندهای مسلّح نامنظم.....حتّی اگر نتوان آنها را به دولتی منتسب کرد، همچنان حملات مسلّحانه هستند.

توصیه‌های سیاست لایدن در مورد مبارزه با تروریسم و حقوق بین‌الملل، از دیدگاه اخیر حمایت و اذعان می کند: «اکنون به خوبی پذیرفته شده که حملات بازیگران غیردولتی، حتّی زمانی که به نمایندگی از یک دولت عمل نمی‌کنند، می‌توانند حمله مسلّحانه محسوب شوند و موجب حقّ دولت در دفاع از خود

disposal and a reluctance to pronounce clearly on matters of contemporary importance." Id.; see David McKeever, The Contribution of the International Court of Justice to the Law on the Use of Force: Missed Opportunities or Unrealistic Expectations? 78 NORDIC J. INT'L L. 361, 396 (2009).

[1]- Judge Kooijmans and Judge Simma

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

گردند»(**Schrijver & Herik; 2010; pp 531, 541-42**). اما در جهت ایجاد تعادل بین دو نظریه مذکور، استین برگ[1]مصالحه معقولی بین آنها برقرار نمود که بنظر می رسد با در نظر گرفتن عملیات دفاع از خود بصورت انفرادی، منعکس کننده عملکرد دولتها است. از نظر وی، پیوند بین بازیگران غیردولتی و یک کشور میزبان باید حداقل در عدم تمایل یا ناتوانی برای توقّف حملات باشد(**Steenberghe, supra note 155. Andrea Bianchi; 2011; pp 197, 202**).[2] این موضع در زمینه تروریسم سایبری، بدان معناست کشورهایی که از حملات تروریستی سایبری(که به آستانه قابل توجّهی می رسند) برخاسته از قلمروشان، سوء استفاده، کنترل، حمایت و یا تحمل می کنند، می توانند با معیارهای تناسب، هدف حمله دولت زیاندیده در مقام دفاع از خود قرار گیرند. اگر حملات از بخش‌هایی از یک کشور ناتوان که دولت ذیربط قادر به کنترل آن نیست، سرچشمه بگیرد، آن مناطق نیز مشمول اقدامات دفاع از خود می‌شوند.

اگرچه بعید بنظر می رسد، اما زمانی که دولتی نمی‌خواهد اقدامات تروریستی سایبری را تحمّل کند؛ مثلاً یک کنوانسیون ضد تروریستی را تصویب کرده و خواستار استرداد یا پیگرد قانونی تروریست می باشد، اما نمی‌تواند عاملان آنرا پیدا کند، ممکن است مشکل ایجاد شود. این امر به ویژه، آنجایی اهمیت می یابد که یک حمله سایبری ویرانگر تنها توسط یک نفر انجام شده باشد و دولت صدمه دیده در صدد انجام عملیات نظامی علیه آن فرد در خاک کشوری باشد که حمله مسلّحانه از قلمرو آن کشور طراحی، برنامه ریزی، مدیریت و اجرا شده باشد. معذالک، اگرچه عملیات نظامی علیه بخش‌هایی از یک کشور، تنها برای تعقیب یک فرد، بی‌سابقه نیست؛ کمااینکه در خصوص اسامه بن لادن[3] رهبر گروه القاعد انجام شد، لیکن با اینحال، ناگزیر پرسش‌هایی را در مورد تناسب بین حمله مهاجم و دفاع از خود در برابر آن و آثار ویرانگر حمله به خاک کشور دیگر، ایجاد می کند. از آنجایی که چنین شرایطی، مشمول قواعد حقوق بین الملل نمی شود، دولت میزبان تنها گزینه رجوع به شورای امنیت را پیش رو دارد که آن هم اگر طرف مقابل، دولتی باشد که دارای حق وتو است، نتیجه ای نخواهد گرفت.

ب- حمله مسلّحانه در تروریسم سایبری

حملات تروریستی سایبری برای اینکه مشمول قواعد حقوقی ناظر به «حمله مسلّحانه» در حقوق مخاصمات گردد، علی القاعده وسعت حمله و آثار مخرّب آن باید به آستانه «حمله مسلّحانه» برسد. لذا کنترل یک پهپاد برای پرواز به داخل ساختمان غیرنظامی، با آنچه در حادثه ۱۱ سپتامبر ۲۰۰۱ در نیویورک رخ داد،

[1]- Steenberghe
[2]- Also see; Military and Paramilitary Activities in and Against Nicaragua, Judgment, 1986 I.C.J 14, ¶ 195 (June 27). It follows that supply of software and “other support” by the host-state will not constitute an “armed attack” itself, however this would make a country a state-sponsor of terror, allowing the victim-state to resort to self-defense (possibly preemptively) against it.
[3]- Osama bin Laden

متفاوت خواهد بود؛ خصوصاً اینکه مبتنی بر منطق اصول قطعنامه ۱۳۶۸ شورای امنیت سازمان ملل متحد، دولت قربانی در مقابل حمله مسلّحانه باید حقّ دفاع از خود را داشته باشد. دیوان بین المللی دادگستری در قضیه گروگانگیری، حملات تهدید کننده به جان پرسنل دیپلماتیک و حمله به آزادی آنها[1] و نیز در قضیه سکوهای نفتی ایران، حمله به کشتی را یک «حمله مسلّحانه» ای که منجر به حقّ دفاع از خود می شود، دانست.[2] دیوان در پرونده تسلیحات هسته‌ای، انتشار تشعشعات اتمی را که آنگاه که بر سلامت، کشاورزی، منابع طبیعی و جمعیت یک منطقه وسیع تأثیر می‌گذارد و می‌تواند به محیط زیست آینده، غذا و اکوسیستم دریایی آسیب برساند و باعث ایجاد نقایص و بیماری های ژنتیکی در نسل های آینده شود، واجد وصف «حمله مسلحانه» دانست.[3]

با اینحال، مواردی از تروریسم سایبری که به آستانه استفاده از زور هم نمی رسد، نمی تواند مشمول موازین حقوقی ناظر به دفاع از خود باشد. مثلاً چنانچه یک سازمان تروریستی از طریق اینترنت اقدام به سرقت وجوه از بانکی کند، از آن جهت که آثار ویرانگری برای یک ملّت یا جمعیت ساکن در یک منطقه جغرافیایی مشخص ندارد و یا محیط زیست و منابع طبیعی یک کشوری را در معرض نابودی قرار نمی دهد، لذا چنین عملیاتی که حتّی به سطح «استفاده از زور» هم نمی رسد، نمی تواند مشمول عنوان «حمله مسلّحانه» موضوع حقوق مخاصمات مسلّحانه قرار بگیرد.

با این همه، بنظر می رسد، این موضوع تا حدودی وابسته به شرایط خاص هر موقعیت و همچنین شرایط سیاسی مربوطه دارد. آنچه ضروری است، حفظ آستانه مطلوب حقوق مخاصمات مسلّحانه برای استناد به حق دفاع از خود در حقوق بین‌الملل می باشد که تحقیقاً آستانه بسیار پایین یک عمل خرابکارانه، موجب زوال مرز بین مخاصمه مسلّحانه برای استناد به حقّ دفاع از خود در مقابل چنین عملی با تعقیب و مجازات مرتکب آن عمل خرابکارانه با استناد به قوانین کیفری می شود(**Kenneth Watkin; 2004; 1–34**)؛ در حالیکه آستانه بالای چنین عملی، از آن جهت که جان انسانها و منافع جمعی یک ملّت و نظم عمومی یک کشور را در معرض خطر قرار می‌دهد، مشمول وصف «حمله مسلّحانه» می شود.

۵- تئوری سوزن یابی[4]

در سال ۱۹۸۹ (پیش از جهانی شدن اینترنت) آنتونیو کاسسه[1] ادعا کرد «از منظر حقوق بین الملل، اقدامات تروریستی برای اینکه واجد شرایط یک حمله مسلّحانه گردد، باید بخشی از یک الگوی ثابت اقدام

[1]- United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶¶ 57, 91 (May 24).
[2]- Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 72 (Nov. 6).
[3]- Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 35 (July 8).
[4]- Needle Pick Theory

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

خشونت‌آمیز باشد نه اینکه فقط حملات منزوی و پراکنده باشد»(**Niaz A. Shah; 2007; pp 95-107**).[۲] حملات سایبری مدرن، پدیده ای کاملاً متفاوت و عمدتاً با اهداف «جدی» بعنوان الگویی مداوم از تلاش برای ورود به یک سیستم با شانس موفقیت نسبتاً کم است.

باید اذعان کرد که وقوع تروریسم سایبری، نه تنها امری غیرممکن نیست، بلکه با توسعه فناوری، امکانپذیرتر هم شده است. اگرچه ممکن است اخفای مواد منفجره در هواپیما بسیار آسان تر از سقوط آن با استفاده از رایانه باشد؛ اما بهره گیری از روشهای پیچیده الکترونیکی با دانش فنّی خاص در فضای سایبر با هدف اثرگذاری بر منافع حیاتی و یا امنیت ملّی و یا ایجاد نا امنی در یک کشور یا منطقه خاص، هدف تروریسم سایبری است. کمااینکه حملات سایبری متعدد به اهداف تصادفی نظیر رایانه های بیمارستانی و تجهیزات پزشکی یک کشور هم می تواند واجد چنین اثر و نتیجه ای باشد؛ در حالیکه در تروریسم سنّتی، برای حصول چنین نتایجی «ممکن است به مجموعه ای از حملات مسلّحانه فیزیکی در قلمرو یک دولت توسط همان گروه تروریستی نیاز باشد(**Bradley K. Ashley; 2003; 34**) »

تئوری سوزن یا نظریه انباشت رویدادها، ناظر به این است که دفاع از خود در قبال حملات تروریستی، حتّی پس از انقضای مدتی از زمان وقوع حمله و خاتمه آن، میسّر و قانونی است. بر اساس این دکترین، بجای اندازه گیری شدّت هر حمله فردی، باید به تأثیر تجمّعی یک سری حملات توجّه شود. به این ترتیب، بجای اینکه حقّ دفاع، بلافاصله پس از انجام یک حمله إعمال شود، اجازه می دهد تا پس از اینکه حمله انجام و منقضی شده نیز از حقّ دفاع از خود در برابر حمله مذکور، استفاده شود. لذا با ابتنای به این تئوری، دولت‌ها اجازه دارند اقدامات قهری لازم برای قطع زنجیره حملات را انجام دهند.(**Tarcisio Gazzini; 2006; pp 319, 331**)

در قضیه سکوهای نفتی، دیوان بین‌المللی دادگستری اشاره کرد که در یک حمله، فعالیت‌های مسلّحانه می‌توانند «ماهیت تجمّعی و تجمیعی»[۳]داشته باشند(**Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 64 Nov. 6**). تعداد زیادی از دولت‌ها، ادعای ترکیه و اسرائیل را از آن جهت که مدعی اند، کراراً درگیر حملات تروریستی در مقیاس کوچک مداوم هستند و حقّ دفاع از خود دارند را مبتنی بر همین تئوری سوزن یا نظریه انباشت رویدادها، بطور ضمنی پذیرفته اند؛[۴] لیکن این تئوری تاکنون، هرگز بطور رسمی

---

[1]- Antonio Cassese
[2]- Niaz A. Shah, Self-Defence, Anticipatory Self-Defence and Pre-Emption: International Law's Response to Terrorism, 12 J. Conflict & Security L. 95, 107 (2007), citing Antonio Cassese, The International Community's "Legal" Response to Terrorism, 38 INT'L & COMP. L. Q. 589, 596 (1989)
[3]- cumulative in character
[4]- Szabó notes that, although the Security Council has been reluctant to accept the needle-prick theory, the Council became less willing to condemn it in the 1980s (particularly in relation to Israeli self-defense wars). See Kinga Tibori Szabo, Anticipatory Action in Self-Defence: Essence and Limits Uuder International Law 215 (2011).

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

توسط شورای امنیت یا علمای برجسته حقوقی و حتّی دیوان بین المللی دادگستری، تأیید نشده است. معذالک، بنظر می رسد از منظر تحلیلی، این تئوری در زمینه تروریسم سایبری نیز از آن جهت که آغازی برای شکل گیری یک رویه بین المللی می باشد، قابل اعتناء است؛ زیرا حداقل دو کشور (ایالات متحده و اسرائیل) در گذشته بطور خاص در پاسخ به اقدامات واجد «اثر تجمّعی»، از قابلیت‌های حمله سایبری جدّی استفاده کرده اند.

حملات تروریستی سایبری در ماهیت خود نسبت به حملات تروریستی سنّتی، شدّت کمتری دارند؛ ضمن آنکه اثرگذاری آنها تا حدود زیادی وابسته به «عامل شانس» طراح و عامل انجام عملیات خرابکارانه در موفقیت و حصول نتیجه مطلوب و موردنظر تروریستها است. بنابراین، احتمال وقوع یک سری حملات مخرّب نظیر الگویی از ترورهای تصادفی از طریق رایانه های پزشکی یا حمل و نقل و یا سوخت رسانی برای نا امن کردن کشور یا جامعه هدف وجود دارد؛ لذا دولت قربانی به توسّل به دکترین سوزن تحریک می شود.

علی ایحالِ نظر به اینکه واکنش متعارف در دفاع از خود در برابر تروریسم سایبری، لاجرم به همان روش رذیلانه صورت می پذیرد تا اقدامی تلافی جویانه بنظر برسد(**Jörg Kammerhofer; 2004; pp 143, 177**) و از آنجا که این رویکرد، تحقیقاً از مرزهای مجاز اقدام پیشگیرانه عبور کرده و احتمالاً بصورت مستقل با حمله سایبری نامتناسب، پاسخ داده خواهد شد؛ با لحاظ اینکه تروریسم سایبری نیز مشمول همان محدودیت‌هایی است که برای دفاع از خود در تروریسم سنّتی از قبیل ضرورت، تناسب، فقدان وسایل دیگر و نیز انقضای حقّ ادامه دفاع از خود پس از آن؛ قابل إعمال است؛ لذا مادام که شورای امنیت یا دیوان بین المللی دادگستری بر مشروع بودن تئوری سوزن، مهر تأیید بزنند و یا تا زمانی که شواهد کافی وجود داشته باشد که نشان دهد این نظریه بصورت عرف بین المللی درآمده، حملات تروریستی سایبری به جز «حمله مسلّحانه»، به صِرف استناد به حملات تجمّعی، نمی تواند محملی برای انجام عملیات تلافی جویانه تحت عنوان دفاع از خود قرار گیرد و بنابراین، کماکان نامشروع خواهد بود.

۳-۱-ضرورت و تناسب

دفاع از خود در برابر اقدامات مخرّب تروریسم سایبری همانند دفاع در قبال حملات مسلّحانه نظامی، مستلزم رعایت اصل ضرورت و تناسب می باشد.

نظر به اینکه حملات تروریستی عمدتاً متشکّل از أعمال غیرقابل پیش‌بینی، ناگهانی و آنی است؛ لذا در پرتو عدم اطمینان قانونی پیرامون تروریسم، تحلیل وضعیت حقوقی دفاع از خود در برابر آن واجد اهمیت

است. بنظر می رسد در مقابله با تروریسم سایبری، ضرورت دارد با قرائتی نو از قواعد حقوقی ناظر به حملات مسلّحانه و دفاع در قبال آن، تفسیری هرمنوتیک از اصول ضرورت و تناسب مورد نظر در اقدامات مربوط به دفاع مشروع در رویکردی جدید بعمل آید. خصوصاً اینکه دولت‌ها در مورد اقداماتی که به راحتی قابل ردیابی نیستند، باید شواهد واضح و قانع‌کننده‌ای مبنی بر لزوم استفاده از زور در دفاع از خود ارائه کنند و ثابت نمایند که چرا افرادی که برخی از آنها هرگز اسلحه در دست نداشتند، باید مورد هدف نظامی قرار گیرند.

تحت عنوان دفاع از خود در برابر تروریسم سایبری، اقدامات «دفاعی» علیه تروریست های سایبری ممکن است شامل اقدامات بحث برانگیز مانند قتل های هدفمند و سریالی[1]و یا اقدامات نوظهور «هک هدفمند یا نظام مند» سیستمهای رایانه ای مانند به دست گرفتن کنترل سامانه های الکترونیکی یا دستکاری سیستم های مخابراتی دشمن، باشد. این اقدامات ممکن است در آینده در چارچوب «جنگ علیه تروریسم سایبری» تحت عنوان اقدامات مقابله ای صورت پذیرد.(**Tarcisio Gazzini; 2006; pp 319, 330**). این امر به ویژه از آن جهت که برخی از دولتها جستجوی از راه دور رایانه‌های مجرمان مشکوک را تجویز کرده اند، حائز مهم است.

البتّه از حیث انجام اقدامات پیش دستانه تحت عنوان اقدامات پیشگیرانه، موضوع نیازمند مداقّه حقوقی است؛ بویژه آنکه «عامل شانس»، تمایز بین پیشگیری از وقوع حمله و دفاع پیش دستانه از خود در مقابله با تروریسم سایبری را زائل می‌کند؛ زیرا پیش‌بینی لحظه حمله سایبری، تقریباً غیرممکن است. بنابراین، توسّل به دفاع از خود پیشگیرانه از نظر قانونی، تنها در صورتی امکانپذیر است که حملات سایبری به شدّت افزایش یابد و احتمالاً با حمله بعدی به سطح «حمله مسلّحانه» برسد، یا چنانچه یک سری حملات سایبری ویرانگر یکسان واقع شده و کماکان در حال انجام است، دولتِ در معرض حمله می داند که احتمالاً در لیست بعدی حمله سایبری قرار دارد.

۶- إعمال قواعد حقوق بشردوستانه بین المللی در برابر سایبر تروریسم

بنظر می رسد حقوق بین‌الملل بشردوستانه[2]به قدر کفایت، جهت ارائه یک «چارچوب نظارتی» و «مکانیسم مؤثر» برای مجازات أعمال تروریستی مناسب است. این نظام حقوقی، اقدامات تروریستی را در

[1] See Peter M. Cullen, The Role of Targeted Killing in the Campaign against Terror, 48 JOINT FORCE Q. 22 (2008); Mary Ellen O'Connell, Defining Armed Conflict, 13 J. CONFLICT & SECURITY L. 393, 400 (2008); Kenneth Anderson, Targeted Killing in U.S. Counterterrorism Strategy and Law 11 (May 11, 2009) (unpublished working paper of the Series on Counterterrorism and American Statutory Law Project with the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution) (on file with author).
[2]-Jjus in Bello

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

مخاصمات بین‌المللی و داخلی محکوم و پیشنهاد می‌کند سیستمی برای تعقیب و مجازات مرتکبین آنها طراحی و تنظیم گردد.(**Luigi Condorelli & Yasmin Naqvi; 37; 2004**).

برخلاف حقوق بشر، نظام حقوق بشردوستانه ماهیت خشونت آمیز یا سیستماتیک أعمال تروریستی انجام شده در طول درگیری ها را در نظر می گیرد؛ اگرچه هر دو نظام حقوقی مذکور در مورد تروریسم و در نتیجه تروریسم سایبری از مجموعه کاستی های خود رنج می برند.(**Fionnuala Ni Aoláin; 2007; 563, 579**).[1] با اینحال، بنظر می رسد مرز بین حمله تروریستی و درگیری مسلّحانه و نتیجتاً امکان استفاده از زور و یا إعمال قواعد حقوق بشردوستانه در برابر آن مبهم است. حمله تروریستی به دلیل ماهیت اقدامات تروریستی، ممکن است بسته به شرایط خاص، آغازی برای یک «درگیری مسلّحانه» باشد. کما اینکه بنظر دیوان بین المللی کیفری برای یوگسلاوی سابق نیز شرط اطلاق درگیری مسلّحانه به یک حمله تروریستی و استفاده از زور در برابر آن، تکرار «اقدام تروریستی» است.[2] بنابراین، صِرف یک حمله تروریستی سایبری به تنهایی نمی تواند آغازگر یک جنگ باشد؛ هرچند بنظر می رسد با تحوّل مفهومی مسئولیت دولتها متعاقب حادثه ۱۱ دسامبر ۲۰۰۱، وقایع پس از این حادثه بطور متناقضی بر عکس آن دلالت دارند.

بهرحال، پیچیدگی‌های مضاعف عملیات‌های ضد تروریسم اخیر («جنگ علیه ترور») نیز از ماهیت بحث‌برانگیز آنها نشأت می‌گیرد و فقط تا حدی با مفهوم کلاسیک جنگ مطابقت دارد. یک حمله تروریستی سایبری می تواند بخشی از یک درگیری مسلّحانه باشد و یا باعث درگیری مسلّحانه شود و به هر روی، آنچه مسلّم است اینکه تروریسم، به اندازه درگیری های مسلّحانه داخلی یا بین المللی ممنوع است(**Hans-Peter Gasser; 2002; pp 547–68**).[3] لذا پروتکل‌های کنوانسیون ژنو نیز که در همان زمان تصویب، بطور خاص با عباراتی نظیر «تمام اقدامات مربوط به تروریسم، «اعمال تروریسم» و«اعمال یا تهدید خشونت آمیز که هدف اصلی آن گسترش ترور در میان مردم غیرنظامی است»[4] را منع و جرم انگاری کردند و یا آراء قضایی دیوان بین المللی کیفری برای یوگسلاوی سابق و یا دادگاه ویژه سیرالئون[5] ولو آنکه با حملات سایبری ارتباط کمی دارند، از آن جهت که عمل افراطی خاص و أعمالی نیز گروگانگیری را ممنوع و جرم

[1]-Also See Gabor Rona, Interesting Times for International Humanitarian Law: Challenges from the “War on Terror”, in Terrorism and Human Rights 154, (Magnus Ranstorp & Paul Wilkinson eds., 2008).
207. Neta C. Crawford, Just War Theory and the U.S. Counterterror War, 1 PERSPECTIVES ON POL. 5, 20 (2003).
[2]- Prosecutor v. Kordić & Čerkez, Case No. IT-95-14/2-A, Appeals Chamber Judgment, ¶ 341 (Int’l Crim. Trib. for the Former Yugoslavia Dec. 17, 2004); See also Prosecutor v. Martić, Case No. IT-95-11-T, Judgment, ¶ 41 n.60 (Int’l Crim. Trib. for the Former Yugoslavia June 12, 2007).
[3]-Also U.N. Secretary-General, A More Secure World: Our Shared Responsibility: Report of the High Level Panel on Threats, Challenges, and Change, ¶ 164(b), U.N. Doc A/59/565 (Dec. 2, 2004).
[4]- Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, art. 4(2)(d), June 10, 1977, 1125 U.N.T.S. 17513 [hereinafter Protocol II].
[5]- U.N. Secretary-General, Report of the Secretary-General on the Establishment of a Special Court for Sierra Leone, art. 3(d), U.N. Doc. S/2000/915 (Oct. 4, 2000).

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

می دانند، دلالت بر آن دارند که با تفسیری هرمنوتیک از همین قواعد حقوق بشردوستانه بین المللی، می توان بیان داشت که تروریسم سایبری نیز بعنوان نوعی عمل خشونت بار و یا تهدیدی خشونت آمیز که هدف اصلی آن گسترش ترور در میان مردم غیرنظامی است، مشمول ممنوعیتهای مقرر می باشند. بنابراین با اتّکای به اسناد بین المللی و رویه قضایی بین المللی، أعمال خشونت آمیز ترور سایبری نیز تابع اصول ضرورت، تناسب، انسانیت، تمایز، بی طرفی و جوانمردی است.

مسلّماً بلحاظ پیشرفت های تکنولوژیکی، امروزه مفهوم کلاسیک تروریسم در حقوق بشردوستانه بین المللی با مفهوم متعارف آن، متفاوت است. زمانی که کنوانسیون های ژنو تدوین شد، جرم انگاری تروریسم بموجب بند ۱ ماده ۳۳ کنوانسیون چهارم ژنو با هدف جلوگیری از «اقدامات ارعاب‌آمیز برای ایجاد رعب و وحشت در میان مردم» توسط متخاصمان صورت پذیرفت.[1]

در رویه قضایی بین المللی بنظر می رسد یک رژیم حقوقی بالفعل مجزا در خصوص کیفیت إعمال قواعد حقوق بشردوستانه نسبت به أعمال تروریستی ایجاد شد. در پرونده گالیچ، دیوان خاطرنشان کرد که اگرچه اسناد بین المللی برای جرم انگاری تروریسم در اشکال مختلف وجود دارد، لیکن دیوان باید خود را به چارچوب قواعد حقوقی ژنو راجع به درگیری های مسلّحانه متعارف بین دولت ها محدود کند.[2] «تلاش‌های «سیاسی» بین‌المللیِ علیه انواع تروریسم ، حاکی است هرگونه حمله سایبری با هدف ایجاد مرگ یا جراحت به غیرنظامیان یا افراد در طول جنگ و درگیری مسلّحانه، نه تنها اگر برای ارعاب مردم انجام شود، بلکه اگر برای وادار کردن یک دولت یا سازمان به انجام یا خودداری از انجام هر عملی استفاده شود، باید یک عمل تروریستی تلقّی شود؛ لیکن اگر هدف خشونت و أعمال غیرخشونت آمیز، صرفاً اجبار حاکمیت یک دولت و نه ارعاب مردم آن کشور باشد، عادلانه و منصفانه نیست که بعنوان تروریسم تلقّی شوند؛ لذا از شمول تعریف مندرج در کنوانسیون تامین مالی تروریسم ۱۹۹۹ خارج شده اند.

به عنوان مثال، ویتک بودن، در حالیکه در جریان حمله سایبری خود در سال ۲۰۰۰، فاضلاب خام را تخلیه می کرد و به اموال و محیط زیست آسیب وارد می کرد، با انگیزه های فردی هدایت می شد و نمی خواست جمعیت را ارعاب کند یا یک دولت یا یک سازمان بین المللی را وادار به انجام کاری بکند.(**Susan W. Brenner; 2006; pp 453, 458**). انجام یا پرهیز از انجام هر عملی، بدون آنکه

[1]- See U.N. Secretary-General, supra note 217, at art. 3(c); Rome Statute of the International Criminal Court, art. 8, 2187 U.N.T.S. 90, July 17, 1998,available at http://www1.umn.edu/humanrts/instree/Rome_Statute_ICC/Rome_ICC_toc.html. Note that negotiations on including "terrorism" as an international crime under the Rome Statute have been underway for more than a decade.
[2]- Emanuela-Chiara Gillard, The Complementary Nature of Human Rights Law, International Humanitarian Law and Refugee Law, in Terrorism and International Law: Challenges and Responses 50 (2002), available at http://www.iihl.org/iihl/ Album/terrorism-law.pdf.

وی قصدی در این زمینه داشته باشد، نمی تواند عمل مجرمانه او را متّصف به وصف تروریسم سایبری نماید.

از آنجایی که حقوق بشردوستانه بین‌المللی اساساً به منظور کنترل رفتار نیروهای نظامی دولتی وضع شده است، لذا حملات سایبری در صورتیکه توسط عوامل نظامی کشورها انجام شوند، کماکان عمل نظامی است و بعید است مشمول مفهوم تروریسم متعارف شوند. این موضوع می تواند در نبردهای مسلّحانه بین‌المللی یا داخلی که گروه‌های سازمان‌یافته بخش‌هایی از قلمرو یک دولت را تحت کنترل خود درآورده اند؛ مصداق داشته باشد. اما افراد و گروه‌هایی که بعنوان رزمنده در میدان نبرد نیستند، چنانچه مرتکب چنین أعمال مجرمانه ای بشوند، به هر حال تحت شمول رژیم حقوقی تروریسم متعارف خواهند بود. این در حالی است که نیروهای نظامی دولتها که بموجب مقررات خاص پروتکل ۲۰۰۵ کنوانسیون دریایی، پروتکل ۲۰۱۰ کنوانسیون تصرف غیرقانونی[1]، کنوانسیون تروریسم هسته ای ۲۰۱۰، کنوانسیون جدید هوانوردی غیرنظامی ۲۰۱۰[2]، فعالیت نظامی انجام می دهند، از این رژیم حقوقی مستثنی هستند.[3]بنابراین، نیروهای نظامی که یک پهپاد غیرنظامی را ربوده و آنرا به ساختمانی می کوبند یا از طریق حملات سایبری در یک درگیری مسلّحانه، باعث تخریب نیروگاه هسته ای کشور دیگری می شوند، مشمول رژیم حقوقی تروریسم متعارف نخواهند بود. (**David J. Bederman; 2010; pp 31, 44**).

النّهایه نتیجه امر هر چه باشد، چنین استثنایی لزوماً مبیّن یک شکاف عمیق قانونی نیست تا مجرا و یا محملی برای رهای از مسئولیت و مجازات قانونی عمل جنایتکارانه باشد؛ زیرا چنین أعمالی همچنان بعنوان جنایات جنگی قابل مجازات هستند و می‌توانند تا حدودی بعنوان تروریسم شناخته شوند، اگرچه شکلی قدیمی از مخاصمات[4] است.

نتیجه

بنظر می رسد با تحلیل کنوانسیون‌های ضد تروریستی، با وجود آنکه برخی از جنایات خارج از محدوده رژیم معاهده باقی می‌مانند، اما همچنان می‌توانند تحت نظام حقوق بین‌الملل عرفی، بعنوان اقدامات تروریستی سایبری تلقّی شوند.

در فناوری، همواره بحث بر سر آن بوده که داده ها توسط انسان طراحی گردیده، اما وجود انسان در داده و داده در انسان محور بحث اصلی است. روزی انسان در داده های اطلاعاتی بود و امروزه داده ها در

[1]- See ICAO, Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft.
[2]- Nuclear Terrorism Convention, at art. 4(2).
[3]- Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, at art. 6(2).
[4]- Jus in Bello.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

انسان. بدن انسان به هیچ وجه مستقیماً به رایانه متصل نیست؛ بنابراین اکثر اقدامات تروریستی سایبری، به استثنای مواردی که منجر پیگیری داده‌های اشتباه توسط انسان به دلیل حمله سایبری می‌شود، از نظر زمانی قبل از آسیب به خود شخص، با ایراد صدمه به اموال و داراییها، منجر به خسارت مالی و اقتصادی می‌شوند.

اتّکای روزافزون به فناوری در کشورهای توسعه‌یافته، همزمان با آسیب‌پذیری شبکه‌های رایانه‌ای، منجر به وضعیتی شده که مجرمان سایبری می‌توانند بین نهادهای مختلفی که در معرض حملات سایبری هستند، از بانک‌ها و مؤسسات مالی گرفته تا سیستم‌های دفاعی نظامی، هر کدام را که هدف است، به آسانی انتخاب کنند.

با این حال، اگرچه همه این حملات تحت تعریف مندرج در پیش نویس کنوانسیون جامع تروریسم بین المللی قرار نمی گیرند؛ لیکن، نشان دهنده اجماع بین دولت ها در اینخصوص، و به این ترتیب، تا حدی انعکاسی از حقوق عرفی است(**Ruwantissa Abeyratne; 2011; pp 337, 340**). در تعریف پیش‌نویس کنوانسیون، از عباراتی نظیر «آسیب جدّی به اموال عمومی یا خصوصی» و «زیان‌های اقتصادی عمده»، استفاده شده که بسیار ذهنی و انتزاعی هستند؛ لیکن می‌توان فهرستی از اشیاء مستعد حملات سایبری تنظیم کرد که ممکن است صِرفاً مبتنی بر شرایط و موقعیت فردی عامل ارتکاب حمله، با «هدف» وادار کردن دولت به انجام یا خودداری از انجام کاری، مورد حمله سایبری قرار بگیرند، در حالیکه هدف وی، ارعاب جمعیت مردمی نباشد. لذا در باب کیفیت إعمال قواعد حقوقی ناظر به تروریسم سایبری، ملاحظاتی مورد توجّه است؛ از جمله اینکه آیا این اولین حمله تروریستی شخص یا گروه تروریستی است، آیا مرتکب عمل تروریستی بدنبال تحقق خواسته ای است، آیا این وضعیت مستحدثه، دارای پس زمینه سیاسی است و غیره. بنابراین، باید بر قصد ارعاب یک جمعیت که احتمالاً از ماهیت و زمینه خود عمل مجرمانه ناشی می شود، تمرکز کرد.

به دلیل ماهیت مجازی بسترهای حملات سایبری، اغلب این حملات، با شکست مواجه می شوند. لذا نمی توان انتظار داشت که خسارات قابل توجّهی به اموال خصوصی مختلف مردم وارد کنند بنحوی که شهروندان عادی را به وحشت و ارعاب بیاندازد. بنابراین، هنگامی که در تروریسم سایبری پیرامون دارایی و ضرر اقتصادی صحبت می شود، منظور حملات سایبری علیه اشیایی نظیر زیرساخت های حیاتی است که برای عملکرد اقتصاد جامعه بعنوان یک کل ضروری هستند و مردم از تخریب و انهدام آنها به وحشت بیفتند. نتیجتاً حملات سایبری که احتمالاً به تأسیسات رایانه ای حیاتی کشاورزی و غذا، آب، بهداشت عمومی، خدمات اضطراری، دولت، مخابرات، انرژی، حمل و نقل، بانک و امور مالی، صنایع شیمیایی و مواد

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

خطرناک، پست و حمل و نقل، پلیس و... آسیب می رساند، باید بموجب قواعد حقوق بین المللی عرفی موجود، اقدامات تروریستی و در نتیجه تروریسم سایبری تلقّی شوند.

بدیهی است که در حملات تروریستی، «مرگ یا آسیب جدّی بدنی»، به خصوص اگر قربانیان تصادفی باشند، هر فرد عادی را بدون توجّه به ابزاری که تروریست ها بکار می گیرند، می ترساند. بنابراین، جدای از أعمال جرم انگاری شده در اسناد بین المللی موجود، حملات سایبری علیه سدها، شبکه های آبرسانی، جایگاه های سوخت و کارخانه های تولید مواد غذایی، شبکه کنترل حمل و نقل زمینی، خودروهای رایانه ای، کنترل های ناوبری هوایی، مؤسسات پزشکی، مواد شیمیایی، آزمایشگاه‌ها و سایر امکانات نیز باید طبق هنجارهای مرسوم، اقدامات تروریستی سایبری در نظر گرفته شوند.

اگرچه سایبرتروریسم در مفهوم نوین و روبه رشد آن، بطور واضح در سطح جهانی جرم انگاری نشده است؛ لیکن چنین اقدامات تروریستی سایبری، مانند سایر أعمال تروریستی و حملات تخریبی که به امنیت ملّی و بین المللی آسیب وارد می آورند، می توانند به عنوان جنایات علیه بشریت، مورد پیگرد قانونی قرار گیرند.

خطر تروریسم سایبری در زمان صلح به اندازه کافی تحت حمایت حقوق بین الملل می باشد و اکنون ضروری است چارچوب قانونی و حقوقی مؤثر و کارامد پیرامون واکنش به این تهدید تعیین گردد تا مشخص شود که آیا چنین اقداماتی به آستانه یک «حمله مسلّحانه» می رسد و آیا دولت ها می توانند با نیروی مسلّح به آن پاسخ دهند یا خیر.

منابع

1. **Abeyratne, Ruwantissa; Cyber Terrorism and Aviation—National and International Responses, 4 J. Trnsp. Security 337, 340 (2011).**
2. **Andrea Bianchi, Terrorism and Armed Conflict: Insights from a Law & Literature Perspective, 24 LEIDEN J. INT'L L. 1, 7 (2011).**
3. **Anna-Maria Talihärm, Cyber Terrorism: in Theory or in Practice? 3.2 Defence Against Terrorism Rev. 59, 62 (2010).**
4. **Bianchi, Andrea; Terrorism and Armed Conflict: Insights from a Law & Literature Perspective, 24 Leiden J. Int'L L. 1, 7 (2011).**
5. **Bill. Nelson, Rodney Choi, Micael Iacobucci, Mark Mitchell & Greg Gagnon, Cyberterror: Prospects and Implications, at IX (1999).cited with approval in Dorothy E. Denning, Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on**

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

Armed Services, U.S. House of Representatives, GEORGETOWN UNIV. (May 23, 2000), http://www.cs.georgetown.edu/~denning/infosec/ cyberterror.html.

6. **Bradley K. Ashley, Anatomy Of Cyberterrorism: Is America Vulnerable? 34 (Feb. 27, 2003) (unpublished research paper submitted for graduation requirements), available at http://www.au.af. mil/au/awc/awcgate/awc/ashley.pdf**
7. **Chesterman, Simon; JUST WAR OR JUST PEACE? Humanitarian Internation and International Law 48 (2001).**
8. **Christine Gray, International Law and the Use of Force 116 (2000).**
9. **Chirstian Henderson, The persistant Advocate and The Use of Force: The Impact of The United States on The Jus Ad Bellum in The Post-Cold War Eea 158 (2010).**
10. **Clay Wilson, Botnets, Cybercrime and Cyberterrorism; Vulnerabilities and Policy Issues for Congress 18 (2008).**
11. **Conway, Maura; Terrorism and IT: Cyberterrorism and Terrorist Organizations Online 6 (2003) (paper prepared for presentation at the International Studies Association Annual International Convention in Portland, Oregon).**
12. **David J. Bederman, Acquiescence, Objection and the Death of Customary International Law, 21 DUKE J. COMP. & INT'L L. 31, 44 (2010)**.
13. **Dennings, Dorothy; A View of Cyberterrorism Five Years Later, in Readings in Internet Security: Hacking, Counterchecking, and Society (K. Himma ed., 2006)**
14. **Dennings, Dorothy E; Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, GEORGETOWN UNIV. (May 23, 2000),**
15. **Derek Jinks; September 11 and the Laws of War, 28 YALE J. INT'L. L. 32 (2003).**
16. **Dobrot, Laurence Andrew; The Global War on Terrorism: A Religious War? STRATEGIC STUD. INST. 6 (2007), available at http://www.strategicstudiesinstitute.army. mil/pdf files/pub822.pdf**
17. **Ellsmore, Nick; Cyber-Terrorism in Australia: The Risk to Business and a Plan to Prepare 7 (2002).**
18. **Emanuela-Chiara Gillard, The Complementary Nature of Human Rights Law, International Humanitarian Law and Refugee Law, in**

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

Terrorism and International Law: Challenges and Responses 50 (2002), available at http://www.iihl.org/iihl/ Album/terrorism-law.pdf

19. **Fionnuala Ni Aoláin, The No-Gaps Approach to Parallel Application in the Context of the War on Terror, 40 ISR. L. REV. 563, 579 (2007)**
20. **Flemming, Peter & Stohl; Michael Myths and Realities of Cyberterrorism, in Countering Terrorism Through International Cooperation: Proceedings of the International Conference 70-105 (Alex P. Schmid ed., 2001).**
21. **Gabor Rona, Interesting Times for International Humanitarian Law: Challenges from the "War on Terror", in Terrorism and Human Rights 154, (Magnus Ranstorp & Paul Wilkinson eds., 2008).**
22. **Gabriel Weimann, Cyberterrorism: How Real Is the Threat? U.S. INST. OF PEACE, Dec. 2004, at 1, 11.**
23. **Gazzini, Tarcisio The Rules on the Use of Force at the Beginning of the XXI Century, 11 J. CONFLICT & SECURITY L. 319, 331 (2006).**
24. **Gillard, Emanuela-Chiara The Complementary Nature of Human Rights Law, International Humanitarian Law and Refugee Law, in Terrorism and International Law: Challenges and Responses 50 (2002), available at http://www.iihl.org/iihl/ Album/terrorism-law.pdf.**
25. **Gordon Sarah & Ford, Richard Cyberterrorism? Symantec (2003)**
26. **Henderson, Chistian; The Persistant Advocate and the Use of Force: The Impact of the United States on the Jus Ad Bellum in the Post-Cold War; Era 158 (2010).**
27. **Hans-Peter Gasser, Acts of Terror, "Terrorism" and International Humanitarian Law, 84 INT'L REV. RED CROSS 547–68 (2002).**
28. **Higgins, Rosalyn; The General International Law of Terrorism, in Terrorism & Int'L L. 28 (Rosalyn Higgins & Maurice Flory eds., 1997)**
29. **Jörg Kammerhofer, Uncertainties of the Law on Self-Defence in the United Nations Charter, 35 NETH. Y.B. INT'L L. 143, 177 (2004).**
30. **Kammerhofer, Jörg Uncertainties of the Law on Self-Defence in the United Nations Charter, 35 NETH. Y.B. INT'L L. 143, 177 (2004).**
31. **Keene, Shima D. Terrorism and the Internet: A Double-Edged Sword, 14 J. Money Laundering Control 359, 364-65 (2011).**
32. **Klang, Mathias; A Critical Look at the Regulation of Computer Viruses, 11 INT'L J. L. & INFO. TECH., 162, 167 (2003).**

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

33. **Kelman, Alistair; The Regulation of Virus Research and the Prosecution for Unlawful Research? 3 J. INFO. L. & TECH. (1997), available at http://elj.warwick. ac.uk/jilt/compcrim/97-3kelm/,**
34. **Kenneth Watkin, Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict, 98 AM. J. INT'L L. 1, 1–34 (2004).**
35. **Krieken, Peter J. Van Terrorism and the International Legal Order; 109 (2002).**
36. **Luigi Condorelli & Yasmin Naqvi, The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of Date?, in Enforcing International Law Norms Against Terrorism ; 37; (2004)**.
37. **Matthew J. Skleroy, *Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Negelect Their Duty to Prevent,* 201 MIL. L. REV. 1, 64-65 (2009)**
38. **McKeever, David The Contribution of the International Court of Justice to the Law on the Use of Force: Missed Opportunities or Unrealistic Expectations? 78 Nordic J. INT'L L. 361, 396 (2009).**
39. **Mauro, Massimo Threat Assessment and Protective Measures: Extending the Asia–Europe Meeting IV Conclusions on Fighting International Terrorism and Other Instruments to Cyber Terrorism, in Cyberwar, Netwar and the Revolution in Military Affairs; 219, 221 (Edward Halpin et al. eds., 2006)**.
40. **Nico Schrijver & Larissa van den Herik, Leiden Policy Recommendations on Counter-terrorism and International Law, 57 NETH. L. REV. 531, 541-42 (2010).**
41. **Peter J. Van Krieken, Terrorism and The International Legal Order 109 (2002).**
42. **Raphaël van Steenberghe, Self-Defense in Response to Attacks by Non-state actors in the Light of Recent State Practice: A Step Forward, 23 Leiden J. Int'L L. 183, 193 (2010).**
43. **Ronen, Yaël Incitement to Terrorist Acts and International Law, 23 Leiden J. INT'L L., 645, 654 (2010)**.
44. **Ruwantissa Abeyratne, Cyber Terrorism and Aviation—National and International Responses, 4 J. TRANSP. SECURITY 337, 340 (2011**.
45. **Sarah Gordon & Richard Ford,*Cyberterrorism?*Stymantec (2003), https://www.symantec.com/avcenter/reference/cyberterrorism.**

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

46. **Shiryaev, Yaroslav; Circumstances Surrounding the Separation Barrier and the Wall Case and Their Relevance for the Right of Self-Defense, 14 GONZ. J. INT'L L. 1 (2010)**
47. **Schrijver Nico & Herik; Larissa van den Leiden Policy Recommendations on Counter-terrorism and International Law, 57 Neth. L. Rev. 531, 541-42 (2010).**
48. **Shah, Niaz A. Self-Defence, Anticipatory Self-Defence and Pre-Emption: International Law's Response to Terrorism, 12 J. Conflict & Security L. 95, 107 (2007),**
49. **Shima D. Keene, Terrorism and the Internet: A Double-Edged Sword, 14 J. Money Laundering Control 359, 364-65 (2011).**
50. **Simona R. Soare, Joe Burton Smart Cities, Cyber Warfare and Social Disorder, [UNDATED].2021.**
51. **Singh Arun Kr. & Siddiqui, Ahmad T. New Face of Terror: Cyber Threats, Emails Containing Viruses, 1 ASIAN J. TECH. & MGMT. RES. (2011) (discussing the new face of terror).**
52. **Skleroy, Matthew J. Solving the Dilemma of State Response to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Negelect Their Duty to Prevent, 201 MIL. L. REV. 1, 64-65 (2009)**
53. **Susan W. Brenner, Cybercrime, Cyberterrorism and Cyberwarfare, 77 REVUE INTERNATIONALE DE DROIT PÉNAL [R.I.D.P.] 453, 458 (2006).**
54. **Starr, Stuart H. Towards and Evolving Theory of Cyberpower, in The Virtual Battlefield: Perspectives on Cyberwarfare, 18, 34 (Christian Czosseck & Kenneth Geers eds., 2009).**
55. **Steenberghe, Raphaël; van Self-Defense in Response to Attacks by Non-state actors in the Light of Recent State Practice: A Step Forward? 23 LEIDEN J. INT'L L. 183, 193 (2010).**
56. **Strobel, W.P. A Glimpse of Cyberwarfare, 128 U.S. News & World Rep. 32 (2000), cited in Joe Wesley Moore, Information Warfare, Cyber-Terrorism and Community Values 24 n.66 (2002) (unpublished LL.M. thesis, McGill University), available at http://www.hsdl.org/?view&did=458383.**
57. **Szabo, Kinga Tibori; Anticipatory Action in Self--Deffence: Essence and Limits Under International Law 215 (2011).**
58. **Tikk, Eneken; Comprehensive Legal Approach to Cyber Security, 35 Dissertations Juridical Universities Tartuensis 22 (2011).**

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال پنجم، شماره نوزدهم، زمستان ۱۴۰۱

59. **Talihärm, Anna-Maria Cyber Terrorism: in Theory or in Practice? 3.2 Defence Against Terrorism Rev. 59, 62 (2010).**
60. **Tarcisio Gazzini, The Rules on the Use of Force at the Beginning of the XXI Century, 11 J. CONFLICT & SECURITY L. 319, 331 (2006).**
61. **Ulfstein, Geir; Terrorism and the Use of Force, 34 Security Dialogue 153, 153-68 (2003).**
62. **Walker, Clive; The Legal Definition of "Terrorism" in United Kingdom Law and Beyond, 2007 PUB. L. 331, 336 (2007).**
63. **Watkin, Kenneth; Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict, 98 AM. J. INT'L L. 1, 1–34 (2004).**
64. **Weimann, Gabriel; Cyberterrorsim: The Sum of All Fears? 28 Stud. In Conflict & Terrorism 129, 130 (2005), cited in Clive Walker, Cyber-Terrorism: Legal Principle and Law in the United Kingdom, 110 PENN ST. L. REV., 625, 634 (2006.)**
65. **Wilson, Clay Botnets; Cybercrime, and Cybertrrorism: Vulnerabilities and Policy Issues for Congress 18 (2008).**
66. **Yaroslav Shiryaev, Circumstances Surrounding the Separation Barrier and the Wall Case and Their Relevance for the Right of Self-Defense, 14 GONZ. J. INT'L L. 1 (2010)**.

Web sites

http://www.un.org/terrorism/instruments.shtml (last visited Aug. 21, 2012).

http://www.cs.georgetown.edu/~denning/infosec/ cyberterror.html

http://www.cs.georgetown.edu/~denning/infosec/ cyberterror.html.

https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

http://www.hsdl.org/?view&did=458383

http://www.gonzagajil.org/index.php?option=com content view=article&id=206: circumstances-surrounding-the-separation-barrier-and-the-wall-case-and-their-relevance-for-the-&catid=83: volume-14-issue-1-2010-2011&Itemid=26

http://www.au.af. mil/au/awc/awcgate/awc/ashley.pdf